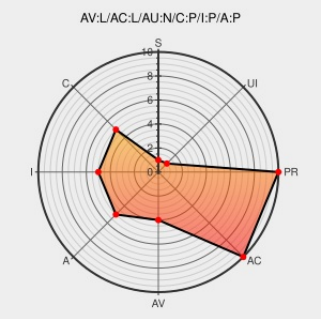
CVE-2009-2653

Published on: 08/03/2009 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:04:00 AM UTC

CVE-2009-2653

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows Server 2003 from Microsoft contain the following vulnerability:

** DISPUTED ** The NtUserConsoleControl function in win32k.sys in Microsoft Windows XP SP2 and SP3, and Server 2003 before SP1, allows local administrators to bypass unspecified "security software" and gain privileges via a crafted call that triggers an overwrite of an arbitrary memory location. NOTE: the vendor disputes the significance of this report, stating that 'the Administrator to SYSTEM "escalation" is not a security boundary we defend.'

CVE-2009-2653 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Microsoft Windows XP (win32k.sys) Local Privilege Escalation Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 9301
笔趣阁_书友最值得收藏的网络小说阅读网	Exploit www.ntinternals.org text/html	MISC www.ntinternals.org/index.html#09_07_30
Security Research & Defense : Latest Baidu public posting requires Adminisrator to elevate	web.archive.org text/html Inactive Link Not Archived	MISC blogs.technet.com/srd/archive/2009/06/11/latest-baidu-public-posting-requires-adminisrator-to-elevate.aspx

如流，新一代智能工作平台	Exploit hi.baidu.com text/html	MISC hi.baidu.com/azy0922/blog/item/f950cbc2890729130ef47783.html
SecurityTracker.com Archives - Windows Kernel win32k.sys Lets Local Users Gain Elevated Privileges	securitytracker.com text/html	SECTRACK 1022630
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 56780

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 Server 2003	All	All	All	All
Operating System	Microsoft	Windows Server 2003	All	All	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

cpe:2.3:o:microsoft:windows_server_2003:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:*:

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 and Source URL Uptime Status status.cve.report