



CVE-2009-2653

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

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

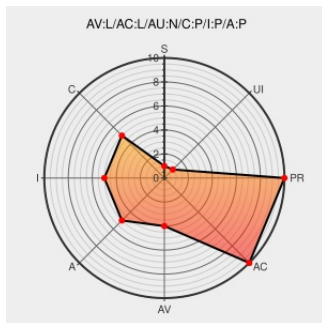
CVE-2009-2653

[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 [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

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 Administrator 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-administrator-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

OSVDB 56780

Inactive Link

Not Archived

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

© [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](#)