



CVE-2010-1895

Published on: 08/11/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:05 PM UTC

CVE-2010-1895

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows 2003 Server](#) from [Microsoft](#) contain the following vulnerability:

The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, do not properly perform memory allocation before copying user-mode data to kernel mode, which allows local users to gain privileges via a crafted application, aka "Win32k Pool Overflow Vulnerability."

CVE-2010-1895 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

COMPLETE

Integrity Impact

COMPLETE

Availability Impact

COMPLETE

CVE References

Description

US-CERT Technical Cyber Security Alert TA10-222A -- Microsoft Updates for Multiple Vulnerabilities

Tags

[US Government Resource](#)
[www.us-cert.gov](#)
[text/xml](#)

Link

[CERT TA10-222A](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL](#)
[oval:org.mitre.oval:def:11844](#)

Microsoft Security Bulletin MS10-048 - Important | Microsoft Docs

[docs.microsoft.com](#)
[text/html](#)

[MS MS10-048](#)

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 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	itanium	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
cpe:2.3:o:microsoft:windows_2003_server:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:*:sp2:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:*:sp2:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:						
cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:						
cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:						

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](#)