



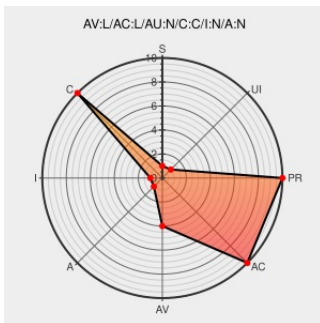
Last Modified on: 03/23/2021 11:28:32 PM UTC

CVE-2013-1248

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Windows 7](#) from [Microsoft](#) contain the following vulnerability:

Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges, and consequently read the

contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.

CVE-2013-1248 has been assigned by  secure@microsoft.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	NONE	NONE

CVE References

Description	Tags	Link
Microsoft Security Bulletin MS13-016 - Important Microsoft Docs	docs.microsoft.com text/html	 MS MS13-016
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:16431
Microsoft Updates for Multiple Vulnerabilities US-CERT	Third Party Advisory US Government Resource www.us-cert.gov text/html	 CERT TA13-043B

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 7	All	All	x64	All
Operating System	Microsoft	Windows 7	All	All	x86	All
Operating System	Microsoft	Windows 7	All	sp1	x64	All
Operating System	Microsoft	Windows 7	All	sp1	x86	All
Operating System	Microsoft	Windows 7	All	All	x64	All
Operating System	Microsoft	Windows 7	All	All	x86	All
Operating System	Microsoft	Windows 7	All	sp1	x64	All
Operating System	Microsoft	Windows 7	All	sp1	x86	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 Server 2008	All	r2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	All	r2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All

System						
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	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_7:*:*:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:x86:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:sp1:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:sp1:x86:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:x86:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:sp1:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:sp1:x86:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2003:*:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2003:*:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:r2:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:r2:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:sp2:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:sp2:x64:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:sp2:x86:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:r2:itanium:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:r2:x64:*:*:*:*:						

cpe:2.3:o:microsoft:windows_server_2008.*:x64.*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008.*:sp2:itanium.*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008.*:sp2:x64.*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008.*:sp2:x86.*:*:*:*:
cpe:2.3:o:microsoft:windows_vista.*:sp2.*:*:*:*:
cpe:2.3:o:microsoft:windows_vista.*:sp2:x64.*:*:*:*:
cpe:2.3:o:microsoft:windows_vista.*:sp2.*:*:*:*:
cpe:2.3:o:microsoft:windows_vista.*:sp2:x64.*:*:*:*:
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

[← Previous ID](#)

Next ID→

© 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