



CVE-2014-0300

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2014-0300
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-12 05:15:19 UTC
Updated	2026-05-06 22:30:45 UTC
Description	win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, and Windows 7 SP1 is susceptible to a buffer overflow attack that could allow a remote attacker to execute arbitrary code on the system. The vulnerability exists in the win32k.sys driver, which is used by the operating system to manage the kernel-mode drivers. The vulnerability is caused by a buffer overflow in the driver's handling of user input, which can be exploited by a remote attacker to execute arbitrary code on the system. The vulnerability affects the following products: Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, and Windows 7 SP1. The vulnerability is rated as Critical (CVSS 7.2) and is tracked by NVD as CVE-2014-0300.

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	-	sp1	All	All

Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References				
Reference	Source		Link	Tags
Microsoft Security Bulletin MS14-015 - Important Microsoft Docs	af854a3a-2127-422b-91ae-364da2661108		docs.microsoft.com	Patch
CVE Program record	CVE.ORG		www.cve.org	canonical
NVD vulnerability detail	NVD		nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.