



# CVE-2011-0677

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

## Summary

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2011-0677                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| State           | PUBLISHED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Assigner        | microsoft                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Published       | 2011-04-13 20:26:25 UTC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Description     | win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows 7 SP1 and SP2 is susceptible to a buffer overflow attack. An attacker who successfully exploits this vulnerability could cause the system to crash or execute arbitrary code. This vulnerability is caused by a buffer overflow in the win32k.sys kernel-mode driver. The vulnerability exists in the win32k.sys kernel-mode driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows 7 SP1 and SP2. An attacker who successfully exploits this vulnerability could cause the system to crash or execute arbitrary code. This vulnerability is caused by a buffer overflow in the win32k.sys kernel-mode driver. |

## 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:** NVD-CWE-Other | 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 2003 Server | All     | sp2    | All     | All      |

|                  |           |                     |     |     |         |     |
|------------------|-----------|---------------------|-----|-----|---------|-----|
| Operating System | Microsoft | Windows 7           | -   | All | All     | All |
| Operating System | Microsoft | Windows 7           | -   | sp1 | x64     | All |
| Operating System | Microsoft | Windows 7           | -   | sp1 | x86     | All |
| Operating System | Microsoft | Windows Server 2003 | All | sp2 | All     | All |
| Operating System | Microsoft | Windows Server 2008 | All | All | itanium | All |
| Operating System | Microsoft | Windows Server 2008 | All | All | x32     | All |
| Operating System | Microsoft | Windows Server 2008 | All | All | x64     | All |
| Operating System | Microsoft | Windows Server 2008 | All | sp2 | x32     | All |
| Operating System | Microsoft | Windows Server 2008 | All | sp2 | x64     | All |
| Operating System | Microsoft | Windows Server 2008 | -   | sp2 | itanium | All |
| Operating System | Microsoft | Windows Server 2008 | r2  | All | itanium | All |
| Operating System | Microsoft | Windows Server 2008 | r2  | All | x64     | All |
| Operating System | Microsoft | Windows Vista       | All | sp1 | All     | All |
| Operating System | Microsoft | Windows Vista       | All | sp2 | All     | All |
| Operating System | Microsoft | Windows Xp          | All | sp3 | All     | All |
| Operating System | Microsoft | Windows Xp          | -   | sp2 | x64     | All |

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

| References                                                                                                             |               |
|------------------------------------------------------------------------------------------------------------------------|---------------|
| Reference                                                                                                              | Source        |
| ASA-2011-110 MS11-034 (2506223)                                                                                        | af854a3a-2127 |
| US-CERT Technical Cyber Security Alert TA11-102A -- Microsoft Updates for Multiple Vulnerabilities                     | af854a3a-2127 |
| MS11-034: Addressing vulnerabilities in the win32k subsystem - Security Research & Defense - Site Home - TechNet Blogs | af854a3a-2127 |
| Microsoft Security Bulletin MS11-034 - Important   Microsoft Docs                                                      | af854a3a-2127 |
| Microsoft Windows Kernel 'Win32k.sys' (CVE-2011-0677) Local Privilege Escalation Vulnerability                         | af854a3a-2127 |
| Microsoft Windows win32k.sys Driver Privilege Escalation Vulnerabilities - Secunia.com                                 | af854a3a-2127 |
| IBM X-Force Exchange                                                                                                   | af854a3a-2127 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                       | af854a3a-2127 |
| Windows Kernel win32k.sys Lets Local Users Gain Elevated Privileges - SecurityTracker                                  | af854a3a-2127 |
| Repository / Oval Repository                                                                                           | af854a3a-2127 |
| CVE Program record                                                                                                     | CVE.ORG       |
| NVD vulnerability detail                                                                                               | NVD           |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)