



# CVE-2015-0057

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-0057                                                                                                                                                                                                                                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                                                                                                                                                                                                                                        |
| <b>Assigner</b>        | secure@microsoft.com                                                                                                                                                                                                                                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                                  |
| <b>Published</b>       | 2015-02-11 03:01:00 UTC                                                                                                                                                                                                                                                                                                                       |
| <b>Updated</b>         | 2019-05-14 18:50:00 UTC                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>     | win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8, Windows 8.1, Windows RT, and Windows RT 8.1 is susceptible to a buffer overflow attack that could allow an attacker to execute arbitrary code or cause a denial of service (DoS) condition. |

## Risk And Classification

### Problem Types: CWE-264

## 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 7           | -       | sp1    | All     | All      |
| Operating System | Microsoft | Windows 8           | -       | All    | All     | All      |
| Operating System | Microsoft | Windows 8           | -       | All    | All     | All      |
| Operating System | Microsoft | Windows 8.1         | -       | 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          | -       | All    | All     | All      |
| Operating System | Microsoft | Windows Rt 8.1      | -       | 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 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 2008 | -       | sp2    | All     | All      |
| Operating System | Microsoft | Windows Server 2008 | r2      | sp1    | All     | All      |

|                  |                           |                                     |    |     |     |     |
|------------------|---------------------------|-------------------------------------|----|-----|-----|-----|
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | r2 | sp1 | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | -  | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | r2 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | -  | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | r2 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | -  | sp2 | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | -  | sp2 | All | All |

## References

| Reference                                                                                             | Source     | Link                                                                                         |
|-------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------|
| Microsoft Windows 8.1 - 'win32k' Local Privilege Escalation (MS15-010) - Windows_x86-64 local Exploit | EXPLOIT-DB | <a href="http://www.exploit-db.com">www.exploit-db.com</a>                                   |
| IBM X-Force Exchange                                                                                  | XF         | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>               |
| Microsoft Windows Kernel 'Win32k.sys' CVE-2015-0057 Local Privilege Escalation Vulnerability          | BID        | <a href="http://www.securityfocus.com/bid/72811">www.securityfocus.com/bid/72811</a>         |
| Microsoft Security Bulletin MS15-010 - Critical   Microsoft Docs                                      | MS         | <a href="https://docs.microsoft.com/en-us/securitybulletins/ms15-010">docs.microsoft.com</a> |
| CVE Program record                                                                                    | CVE.ORG    | <a href="http://www.cve.org">www.cve.org</a>                                                 |
| NVD vulnerability detail                                                                              | NVD        | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                               |

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)