



# CVE-2010-0232

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

## Summary

|                        |                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-0232                                                                                                    |
| <b>State</b>           | PUBLIC                                                                                                           |
| <b>Assigner</b>        | secure@microsoft.com                                                                                             |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                     |
| <b>Published</b>       | 2010-01-21 19:30:00 UTC                                                                                          |
| <b>Updated</b>         | 2023-12-07 18:38:00 UTC                                                                                          |
| <b>Description</b>     | The kernel in Microsoft Windows NT 3.1 through Windows 7, including Windows 2000 SP4, Windows XP SP2 and SP3, Wi |

## Risk And Classification

**EPSS:** 0.726210000 probability, percentile 0.987750000 (date 2026-04-17)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** CWE-264

## CISA Known Exploited Vulnerability

|                        |                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Vendor</b>          | Microsoft                                                                                                   |
| <b>Product</b>         | Windows                                                                                                     |
| <b>Name</b>            | Microsoft Windows Kernel Exception Handler Vulnerability                                                    |
| <b>Required Action</b> | Apply updates per vendor instructions.                                                                      |
| <b>Notes</b>           | <a href="https://nvd.nist.gov/vuln/detail/CVE-2010-0232">https://nvd.nist.gov/vuln/detail/CVE-2010-0232</a> |

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                             | Version | Update | Edition | Language |
|------------------|---------------------------|-------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 2000</a>        | sp4     | All    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 2000</a>        | sp4     | All    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 7</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 7</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Nt</a>          | 3.1     | All    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Nt</a>          | 3.1     | All    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2003</a> | All     | sp2    | All     | All      |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2003</a> | All     | sp2    | All     | All      |

|                  |                           |                                     |     |     |         |     |
|------------------|---------------------------|-------------------------------------|-----|-----|---------|-----|
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | All | itanium | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | All | x32     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | All | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | sp2 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | -   | sp2 | itanium | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | sp2 | x32 | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | All | itanium | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | All | x32     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | All | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | All | sp2 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | -   | sp2 | itanium | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> | sp2 | x32 | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | All | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | sp1 | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | sp1 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | sp2 | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | sp2 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | sp1 | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | sp2 | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | All | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | sp1 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | All | sp2 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | sp1 | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Vista</a>       | sp2 | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | -   | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | -   | sp2 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | sp3 | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | -   | All | All     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | -   | sp2 | x64     | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | sp3 | All | All     | All |

| Reference        | Source                    | Link                                |
|------------------|---------------------------|-------------------------------------|
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2008</a> |

|                                                                                                                                                        |          |                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------|
| SecurityFocus                                                                                                                                          | BUGT/HAQ | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |
| Full Disclosure: Microsoft Windows NT #GP Trap Handler Allows Users to Switch Kernel Stack                                                             | FULLDISC | <a href="http://seclists.org">seclists.org</a>                                 |
| Microsoft Security Advisory (979682): Vulnerability in Windows Kernel Could Allow Elevation of Privilege                                               | CONFIRM  | <a href="http://www.microsoft.com">www.microsoft.com</a>                       |
| US-CERT Technical Cyber Security Alert TA10-040A -- Microsoft Updates for Multiple Vulnerabilities                                                     | CERT     | <a href="http://www.us-cert.gov">www.us-cert.gov</a>                           |
| <a href="http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip">lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip</a> | MISC     | <a href="http://lock.cmpxchg8b.com">lock.cmpxchg8b.com</a>                     |
| The Microsoft Security Response Center (MSRC) : Security Advisory 979682 Released                                                                      | CONFIRM  | <a href="http://blogs.technet.com">blogs.technet.com</a>                       |
| [dailydave] 20100119 We hold these axioms to be self evident                                                                                           | MLIST    | <a href="http://lists.immunitysec.com">lists.immunitysec.com</a>               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                                       | VUPEN    | <a href="http://www.vupen.com">www.vupen.com</a>                               |
| Repository / Oval Repository                                                                                                                           | OVAL     | <a href="http://oval.cisecurity.org">oval.cisecurity.org</a>                   |
| Windows Kernel #GP Trap Handler Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker                                                       | SECTrack | <a href="http://securitytracker.com">securitytracker.com</a>                   |
| Microsoft Windows Two Privilege Escalation Vulnerabilities - Advisories - Community                                                                    | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                                   |
| IBM X-Force Exchange                                                                                                                                   | XF       | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |
| Microsoft Windows #GP Trap Handler Local Privilege Escalation Vulnerability                                                                            | BID      | <a href="http://www.securityfocus.com/bid">www.securityfocus.com/bid</a>       |
| Microsoft Security Bulletin MS10-015 - Important   Microsoft Docs                                                                                      | MS       | <a href="http://docs.microsoft.com">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>                                 |
| CISA Known Exploited Vulnerabilities catalog                                                                                                           | CISA     | <a href="http://www.cisa.gov">www.cisa.gov</a>                                 |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**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)