



# CVE-2006-1311

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

## Summary

|                        |                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2006-1311                                                                                                    |
| <b>State</b>           | PUBLIC                                                                                                           |
| <b>Assigner</b>        | secure@microsoft.com                                                                                             |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                     |
| <b>Published</b>       | 2007-02-13 20:28:00 UTC                                                                                          |
| <b>Updated</b>         | 2018-10-12 21:39:00 UTC                                                                                          |
| <b>Description</b>     | The RichEdit component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1; Office 2000 SP3, XP SP3, 2003 SP2, a |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor    | Product             | Version | Update | Edition | Language |
|------------------|-----------|---------------------|---------|--------|---------|----------|
| Application      | Microsoft | Learning Essentials | 1.0     | All    | All     | All      |
| Application      | Microsoft | Learning Essentials | 1.1     | All    | All     | All      |
| Application      | Microsoft | Learning Essentials | 1.5     | All    | All     | All      |
| Application      | Microsoft | Learning Essentials | 1.0     | All    | All     | All      |
| Application      | Microsoft | Learning Essentials | 1.1     | All    | All     | All      |
| Application      | Microsoft | Learning Essentials | 1.5     | All    | All     | All      |
| Application      | Microsoft | Office              | All     | All    | All     | All      |
| Application      | Microsoft | Office              | 2000    | sp3    | All     | All      |
| Application      | Microsoft | Office              | 2003    | sp2    | All     | All      |
| Application      | Microsoft | Office              | xp      | sp3    | All     | All      |
| Application      | Microsoft | Office              | All     | All    | All     | All      |
| Application      | Microsoft | Office              | 2000    | sp3    | All     | All      |
| Application      | Microsoft | Office              | 2003    | sp2    | All     | All      |
| Application      | Microsoft | Office              | xp      | sp3    | All     | All      |
| Operating System | Microsoft | Windows 2000        | All     | sp4    | All     | fr       |
| Operating System | Microsoft | Windows 2000        | All     | sp4    | All     | fr       |
| Operating System | Microsoft | Windows 2003 Server | sp1     | All    | All     | All      |

|                  |                           |                                     |     |     |           |     |
|------------------|---------------------------|-------------------------------------|-----|-----|-----------|-----|
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 2003 Server</a> | sp1 | All | All       | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | All | sp2 | tablet_pc | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Xp</a>          | All | sp2 | tablet_pc | All |

## References

| Reference                                                                                                         | Source   | Link                                         |
|-------------------------------------------------------------------------------------------------------------------|----------|----------------------------------------------|
| Microsoft RichEdit OLE Dialog Memory Corruption Vulnerability - Advisories - Secunia                              | SECUNIA  | <a href="#">secunia.com</a>                  |
| Microsoft Windows RichEdit OLE Memory Corruption Error Lets Remote Users Execute Arbitrary Code - SecurityTracker | SECTRACK | <a href="#">www.securitytracker.com</a>      |
| US-CERT Technical Cyber Security Alert TA07-044A -- Microsoft Updates for Multiple Vulnerabilities                | CERT     | <a href="#">www.cisa.gov</a>                 |
| Repository / Oval Repository                                                                                      | OVAL     | <a href="#">oval.fedoraproject.org</a>       |
| Microsoft Office And Microsoft Windows RichEdit Component Remote Code Execution Vulnerability                     | BID      | <a href="#">www.bidsa.org</a>                |
| 31886                                                                                                             | OSVDB    | <a href="#">www.osvdb.org</a>                |
| US-CERT Vulnerability Note VU#368132                                                                              | CERT-VN  | <a href="#">www.cisa.gov</a>                 |
| Microsoft Security Bulletin MS07-013 - Important   Microsoft Docs                                                 | MS       | <a href="#">docs.microsoft.com</a>           |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                  | VUPEN    | <a href="#">www.vulnhub.com</a>              |
| IBM X-Force Exchange                                                                                              | XF       | <a href="#">exchange.xforce.ibmcloud.com</a> |
| Microsoft Office OLE Memory Corruption Error Lets Remote Users Execute Arbitrary Code - SecurityTracker           | SECTRACK | <a href="#">www.securitytracker.com</a>      |
| CVE Program record                                                                                                | CVE.ORG  | <a href="#">www.cve.org</a>                  |
| NVD vulnerability detail                                                                                          | NVD      | <a href="#">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](#)

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