



CVE-2003-0109

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2003-0109 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2003-03-31 05:00:00 UTC |
| Updated | 2023-11-07 01:56:00 UTC |
| Description | Buffer overflow in ntdll.dll on Microsoft Windows NT 4.0, Windows NT 4.0 Terminal Server Edition, Windows 2000, and Win |

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-----------|--------------------------------|---------|--------|---------|----------|
| Operating System | Microsoft | Windows 2000 | All | All | All | All |
| Operating System | Microsoft | Windows 2000 | All | sp1 | All | All |
| Operating System | Microsoft | Windows 2000 | All | sp2 | All | All |
| Operating System | Microsoft | Windows 2000 | All | sp3 | All | All |
| Operating System | Microsoft | Windows 2000 | All | All | All | All |
| Operating System | Microsoft | Windows 2000 | All | sp1 | All | All |
| Operating System | Microsoft | Windows 2000 | All | sp2 | All | All |
| Operating System | Microsoft | Windows 2000 | All | sp3 | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | All | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | sp1 | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | sp2 | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | sp3 | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | All | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | sp1 | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | sp2 | All | All |
| Operating System | Microsoft | Windows 2000 Terminal Services | All | sp3 | All | All |

References

| Reference | Source | Link |
|---|-----------|------------------------------|
| Microsoft Support | | support.mic |
| nextgenss.com - This website is for sale! - nextgenss Resources and Information. | MISC | www.nextge |
| CERT Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL | CERT | www.cert.or |
| 'New attack vectors and a vulnerability dissection of MS03-007' - MARC | BUGTRAQ | marc.info |
| 'WDAV exploit without netcat and with pretty magic number' - MARC | BUGTRAQ | marc.info |
| Microsoft Security Bulletin MS03-007 - Critical Microsoft Docs | MS | docs.micros |
| 'IIS 5.0 WebDAV -Proof of concept-. Fully documented.' - MARC | BUGTRAQ | marc.info |
| Download details: Windows 2000 Security Patch: IIS Remote Exploit from ntdll.dll Vulnerability | CONFIRM | microsoft.cc |
| 'WebDAV exploit: using wide character decoder scheme' - MARC | BUGTRAQ | marc.info |
| 20030317 Microsoft IIS WebDAV Remote Compromise Vulnerability | ISS | www.iss.ne |
| 'Fate Research Labs Presents: Analysis of the NTDLL.DLL Exploit' - MARC | BUGTRAQ | marc.info |
| Repository / Oval Repository | OVAL | oval.cisecu |
| Microsoft Support | MSKB | support.mic |
| CERT/CC Vulnerability Note VU#117394 | CERT-VN | www.kb.cer |
| ISS X-Force Database: http-webdav-long-request (11533): Microsoft IIS WebDAV long request buffer overflow | XF | www.iss.ne |
| Microsoft Windows ntdll.dll Buffer Overflow Vulnerability | BID | www.securi |
| 'New attack vectors and a vulnerability dissection of MS03-007' - MARC | NTBUGTRAQ | marc.info |
| CVE Program record | CVE.ORG | www.cve.or |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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](#).

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