



CVE-2010-0625

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2010-0625 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2010-04-05 16:30:00 UTC |
| Updated | 2018-10-10 19:53:00 UTC |
| Description | Stack-based buffer overflow in NWFTPD.nlm before 5.10.01 in the FTP server in Novell NetWare 5.1 through 6.5 SP8 allow |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------|---------|--------|---------|----------|
| Operating System | Novell | Netware | 5.1 | All | All | All |
| Operating System | Novell | Netware | 5.1 | sp2a | All | All |
| Operating System | Novell | Netware | 5.1 | sp3 | All | All |
| Operating System | Novell | Netware | 5.1 | sp4 | All | All |
| Operating System | Novell | Netware | 5.1 | sp6 | All | All |
| Operating System | Novell | Netware | 6.0 | All | All | All |
| Operating System | Novell | Netware | 6.0 | sp1 | All | All |
| Operating System | Novell | Netware | 6.0 | sp2 | All | All |
| Operating System | Novell | Netware | 6.0 | sp3 | All | All |
| Operating System | Novell | Netware | 6.5 | All | All | All |
| Operating System | Novell | Netware | 6.5 | sp1 | All | All |
| Operating System | Novell | Netware | 6.5 | sp1.1a | All | All |
| Operating System | Novell | Netware | 6.5 | sp1.1b | All | All |
| Operating System | Novell | Netware | 6.5 | sp2 | All | All |
| Operating System | Novell | Netware | 6.5 | sp3 | All | All |
| Operating System | Novell | Netware | 6.5 | sp4 | All | All |
| Operating System | Novell | Netware | 6.5 | sp5 | All | All |

| | | | | | | |
|------------------|--------|--------------------|---------|--------|-----|-----|
| Operating System | Novell | Netware | 6.5 | sp6 | All | All |
| Operating System | Novell | Netware | 6.5 | sp7 | All | All |
| Operating System | Novell | Netware | 6.5 | sp8 | All | All |
| Operating System | Novell | Netware | 5.1 | All | All | All |
| Operating System | Novell | Netware | 5.1 | sp2a | All | All |
| Operating System | Novell | Netware | 5.1 | sp3 | All | All |
| Operating System | Novell | Netware | 5.1 | sp4 | All | All |
| Operating System | Novell | Netware | 5.1 | sp6 | All | All |
| Operating System | Novell | Netware | 6.0 | All | All | All |
| Operating System | Novell | Netware | 6.0 | sp1 | All | All |
| Operating System | Novell | Netware | 6.0 | sp2 | All | All |
| Operating System | Novell | Netware | 6.0 | sp3 | All | All |
| Operating System | Novell | Netware | 6.5 | All | All | All |
| Operating System | Novell | Netware | 6.5 | sp1 | All | All |
| Operating System | Novell | Netware | 6.5 | sp1.1a | All | All |
| Operating System | Novell | Netware | 6.5 | sp1.1b | All | All |
| Operating System | Novell | Netware | 6.5 | sp2 | All | All |
| Operating System | Novell | Netware | 6.5 | sp3 | All | All |
| Operating System | Novell | Netware | 6.5 | sp4 | All | All |
| Operating System | Novell | Netware | 6.5 | sp5 | All | All |
| Operating System | Novell | Netware | 6.5 | sp6 | All | All |
| Operating System | Novell | Netware | 6.5 | sp7 | All | All |
| Operating System | Novell | Netware | 6.5 | sp8 | All | All |
| Application | Novell | Netware Ftp Server | 5.01i | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01o | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01w | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01y | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02b | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02i | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02r | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02y | All | All | All |
| Application | Novell | Netware Ftp Server | 5.03b | All | All | All |
| Application | Novell | Netware Ftp Server | 5.03l | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.20 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.25 | All | All | All |

| | | | | | | |
|-------------|--------|--------------------|---------|-----|-----|-----|
| Application | Novell | Netware Ftp Server | 5.04.5 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.8 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.05 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.05.04 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.06.04 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.06.05 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.07 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.07.02 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01i | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01o | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01w | All | All | All |
| Application | Novell | Netware Ftp Server | 5.01y | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02b | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02i | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02r | All | All | All |
| Application | Novell | Netware Ftp Server | 5.02y | All | All | All |
| Application | Novell | Netware Ftp Server | 5.03b | All | All | All |
| Application | Novell | Netware Ftp Server | 5.03l | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.20 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.25 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.5 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.04.8 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.05 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.05.04 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.06.04 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.06.05 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.07 | All | All | All |
| Application | Novell | Netware Ftp Server | 5.07.02 | All | All | All |

References

| Reference | Source | Link |
|--|---------|--|
| About Secunia Research Flexera | SECUNIA | secunia.cc |
| SecurityFocus | BUGTRAQ | www.secu |
| Advisories | MISC | www.prote |
| What fixes are in NWFTPD.NLM v5.10.01, March 26, 2010? | CONFIRM | www.nove |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | www.vupe |

| | | |
|---|----------|-----------------------------|
| Access Denied | CONFIRM | bugzilla.nc |
| Novell Netware FTP Server Multiple Commands Remote Buffer Overflow Vulnerabilities | BID | www.secu |
| SecurityFocus | BUGTRAQ | www.secu |
| Zero Day Initiative | MISC | www.zeroc |
| NetWare FTP Server Buffer Overflow Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker | SECTRACK | securitytra |
| CVE Program record | CVE.ORG | www.cve.c |
| NVD vulnerability detail | NVD | nvd.nist.gc |

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](#)