



CVE-2004-2767

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

Summary

CVE	CVE-2004-2767
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-04-05 15:30:00 UTC
Updated	2010-04-06 04:00:00 UTC
Description	NWFTPD.nlm before 5.04.25 in the FTP server in Novell NetWare does not promptly close DS sessions, which allows remote users to execute arbitrary commands and cause a denial of service (DoS) by crashing the server. The vulnerability exists because the server does not properly validate the length of the session ID. This vulnerability is related to CVE-2004-2766.

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Novell	Netware	All	All	All	All
Operating System	Novell	Netware	All	All	All	All
Application	Novell	Netware Ftp Server	All	All	All	All
Application	Novell	Netware Ftp Server	All	All	All	All

References

Reference	Source	Link	Tags
What fixes are in NWFTPD.NLM v5.10.01, March 26, 2010?	CONFIRM	www.novell.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)