



CVE-2007-1080

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

Summary

CVE	CVE-2007-1080
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-22 23:28:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Multiple heap-based buffer overflows in TurboFTP 5.30 Build 572 allow remote servers to cause a denial of service via (1) I

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Turbosoft	Turboftp	5.3.0	build_572	All	All
Application	Turbosoft	Turboftp	5.3.0	build_572	All	All

References

Reference	Source	Li
IBM X-Force Exchange	XF	e>
33782	OSVDB	os
TurboFTP Denial Of Service And Buffer Overflow Vulnerabilities	BID	w
TurboFTP Server 5.30 Build 572 - 'newline/LIST' Multiple Remote Denial of Service Vulnerabilities - Windows dos Exploit	EXPLOIT-DB	w
33752	OSVDB	os
IBM X-Force Exchange	XF	e>
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

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](#)