



CVE-2014-1441

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

Summary

CVE	CVE-2014-1441
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-02 01:59:00 UTC
Updated	2014-05-02 15:11:00 UTC
Description	Core FTP Server 1.2 before build 515 allows remote attackers to cause a denial of service (reachable assertion and crash)

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coreftp	Core Ftp	1.2	All	All	All
Application	Coreftp	Core Ftp	1.2	All	All	All

References

Reference	Source
Core FTP Server 1.2 DoS / Traversal / Disclosure ≈ Packet Storm	MISC
102966	OSVDB
Security vulnerability, updated builds - Core FTP	CONFIRMED
Full Disclosure: Core FTP Server Vulnerabilities	FULLDISCLOSURE
Security Advisory SA56850 - Core FTP Server / SFTP Server Information Disclosure and Denial of Service Vulnerabilities - Secunia	SECURITYADVISORY
CVE Program record	CVE.Org
NVD vulnerability detail	NVD

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](#)