

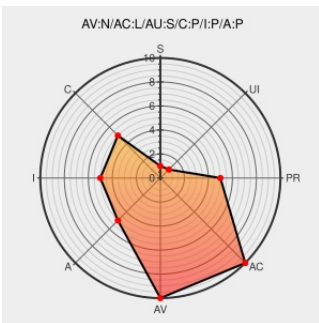


CVE-2004-2523

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2523

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openftpd Ftp Server](#) from [Openftpd](#) contain the following vulnerability:

Format string vulnerability in the msg command (cat_message function in msg.c) in OpenFTPD 0.30.2 and earlier allows remote authenticated users to execute arbitrary code via format string specifiers in the message argument.

CVE-2004-2523 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

OpenFTPD: Welcome

Tags

[web.archive.org](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

Link

[CONFIRM](#)

www.openftpd.org:9673/openftpd

No Description Provided

[Patch](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

[BUGTRAQ 20040729 \[VSA0402\]](#)
[OpenFTPD format string vulnerability](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

[text/html](#)

[XF openftpd-ncftpformat-string\(16843\)](#)

Secunia - Advisories - OpenFTPD "SITE MSG" FTP Command
Format String Vulnerability

[Patch](#)

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[SECUNIA 12174](#)

Exploit
archives.neohapsis.com
text/x-c
Inactive Link Not Archived

BUGTRAQ 20040803 EXPLOIT for Re: [VSA0402] OpenFTPD format string vulnerability

SecurityTracker.com Archives - OpenFTPD Format String Flaw Lets Remote Authenticated Users Execute Arbitrary Code

Exploit
Patch
securitytracker.com
text/html

SECTrack 1010823

No Description Provided

www.osvdb.org
Inactive Link Not Archived

OSVDB 8261

OpenFTPD Remote Message Format String Vulnerability

Exploit
Patch
cve.report (archive)
text/html

BID 10830

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openftpd	Openftpd Ftp Server	0.29.4	All	All	All
Application	Openftpd	Openftpd Ftp Server	0.30	All	All	All
Application	Openftpd	Openftpd Ftp Server	0.30.1	All	All	All
Application	Openftpd	Openftpd Ftp Server	All	All	All	All
Application	Openftpd	Openftpd Ftp Server	0.29.4	All	All	All
Application	Openftpd	Openftpd Ftp Server	0.30	All	All	All
Application	Openftpd	Openftpd Ftp Server	0.30.1	All	All	All

cpe:2.3:a:openftpd:openftpd_ftp_server:0.29.4:*:*:*:*:*:

cpe:2.3:a:openftpd:openftpd_ftp_server:0.30:*:*:*:*:*:

cpe:2.3:a:openftpd:openftpd_ftp_server:0.30.1:*:*:*:*:*:

cpe:2.3:a:openftpd:openftpd_ftp_server:*:*:*:*:*:

cpe:2.3:a:openftpd:openftpd_ftp_server:0.29.4:*:*:*:*:*:

cpe:2.3:a:openftpd:openftpd_ftp_server:0.30:*:*:*:*:*:

cpe:2.3:a:openftpd:openftpd_ftp_server:0.30.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#)