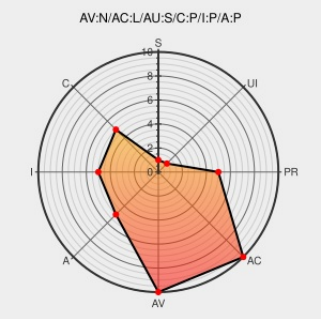
CVE-2004-2523

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
OpenFTPD: Welcome	web.archive.org, text/html, Inactive Link, Not Archived	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

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

← Previous ID

Next ID→