

Print: PDF

Reference	Source	Link
FSPLIB Library Multiple Remote Vulnerabilities	BID	www.securityfocus.com/bid/23447
gFTP Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com/advisories/23447
38569	OSVDB	osvdb.org/38569
Gentoo Linux Documentation -- gFTP: Multiple vulnerabilities	GENTOO	security.gentoo.org/gentoo-sources/gftp
fsplib Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com/advisories/23447
Gentoo Bug 188252 - net-ftp/gftp < 2.0.18-r6 uses vulnerable fsplib code (CVE-2007-3961, CVE-2007-3962)	CONFIRM	bugs.gentoo.org/188252
38570	OSVDB	osvdb.org/38570
CVS Info for project fsp	MISC	fsp.cvs.sourceforge.net
CVS Info for project fsp	CONFIRM	fsp.cvs.sourceforge.net
CVS Info for project fsp	MISC	fsp.cvs.sourceforge.net
Support / Security / Advisories / / MDVSA-2008:018 Mandriva	MANDRIVA	www.mandriva.com/en/Security/Advisories/MDVSA-2008:018
Gentoo update for gftp - Advisories - Secunia	SECUNIA	secunia.com/advisories/23447
CVE Program record	CVE.ORG	www.cve.org

NVD vulnerability detailNVDnvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-08-10	Mark J Cox	Not vulnerable. fsplib is part of gftp in Red Hat Enterprise Linux 5, but this issue does not affect I

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](#)