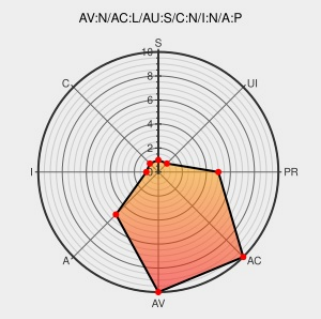
CVE-2008-7264

Published on: 10/19/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:14 PM UTC

CVE-2008-7264

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pyftpdlib from G.rodola contain the following vulnerability:

The ftp_QUIT function in ftpserver.py in pyftpdlib before 0.5.0 allows remote authenticated users to cause a denial of service (file descriptor exhaustion and daemon outage) by sending a QUIT command during a disallowed data-transfer attempt.

CVE-2008-7264 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
GitHub - giampaolo/pyftpdlib: Extremely fast and scalable Python FTP server library	code.google.com text/html	CONFIRM code.google.com/p/pyftpdlib/source/detail?r=344
GitHub - giampaolo/pyftpdlib: Extremely fast and scalable Python FTP server library	code.google.com text/html	CONFIRM code.google.com/p/pyftpdlib/source/diff?spec=svn344&r=344&format=side&path=/trunk/pyftpdlib/ftpserver.py
HISTORY - pyftpdlib - Project Hosting on Google Code	code.google.com text/html	CONFIRM code.google.com/p/pyftpdlib/source/browse/trunk/HISTORY
Socket handles are leaked when a data transfer is in progress and user QUITs · Issue #71 · giampaolo/pyftpdlib · GitHub	Exploit Patch code.google.com text/html	CONFIRM code.google.com/p/pyftpdlib/issues/detail?id=71

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	G.rodola	Pyftpdlib	0.1	All	All	All
Application	G.rodola	Pyftpdlib	0.1.1	All	All	All
Application	G.rodola	Pyftpdlib	0.2.0	All	All	All
Application	G.rodola	Pyftpdlib	0.3.0	All	All	All
Application	G.rodola	Pyftpdlib	All	All	All	All
Application	G.rodola	Pyftpdlib	0.1	All	All	All
Application	G.rodola	Pyftpdlib	0.1.1	All	All	All
Application	G.rodola	Pyftpdlib	0.2.0	All	All	All
Application	G.rodola	Pyftpdlib	0.3.0	All	All	All

cpe:2.3:a:g.rodola:pyftpdlib:0.1:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:*:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.1:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:g.rodola:pyftpdlib:0.3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© 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 registred 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