



CVE-2009-5012

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

Last Modified on: 03/23/2021 11:25:28 PM UTC

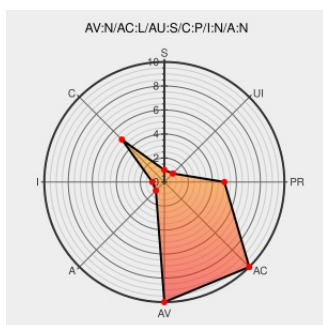
CVE-2009-5012

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Pyftplib](#) from [G.rodola](#) contain the following vulnerability:

ftpsrvr.py in pyftplib before 0.5.2 does not require the l permission for the MLST command, which allows remote authenticated users to bypass intended access restrictions and list the root directory via an FTP session.

CVE-2009-5012 has been assigned by [M](#) 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

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

"l" permission should be valid also for MLST command · Issue #114 · giampaolo/pyftplib · GitHub

[code.google.com](#)
[text/html](#)

[CONFIRM code.google.com/p/pyftplib/issues/detail?id=114](#)

GitHub - giampaolo/pyftplib: Extremely fast and scalable Python FTP server library

[code.google.com](#)
[text/html](#)

[CONFIRM code.google.com/p/pyftplib/source/detail?r=596](#)

HISTORY - pyftplib - Project Hosting on Google Code

[code.google.com](#)
[text/html](#)

[CONFIRM code.google.com/p/pyftplib/source/browse/trunk/HISTORY](#)

GitHub - giampaolo/pyftplib: Extremely fast and scalable Python FTP server library

[code.google.com](#)
[text/html](#)

[CONFIRM code.google.com/p/pyftplib/source/diff?spec=svn596&r=596&format=side&path=/trunk/pyftplib/ftpsrvr.py](#)

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

This report does not endorse any commercial products that may be mentioned in these sheets. Please address comments about any missed 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	Pyftplib	0.1	All	All	All
Application	G.rodola	Pyftplib	0.1.1	All	All	All
Application	G.rodola	Pyftplib	0.2.0	All	All	All
Application	G.rodola	Pyftplib	0.3.0	All	All	All
Application	G.rodola	Pyftplib	0.4.0	All	All	All
Application	G.rodola	Pyftplib	0.5.0	All	All	All
Application	G.rodola	Pyftplib	All	All	All	All
Application	G.rodola	Pyftplib	0.1	All	All	All
Application	G.rodola	Pyftplib	0.1.1	All	All	All
Application	G.rodola	Pyftplib	0.2.0	All	All	All
Application	G.rodola	Pyftplib	0.3.0	All	All	All
Application	G.rodola	Pyftplib	0.4.0	All	All	All
Application	G.rodola	Pyftplib	0.5.0	All	All	All

```
cpe:2.3:a:g.rodola:pyftplib:0.1:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.2.0:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.4.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.5.0:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:*.:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.1:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.2.0:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.3.0:*.:*:*:*:*:*:
```

```
cpe:2.3:a:g.rodola:pyftplib:0.4.0:*:*:*:*:*:*:
```

cpe:2.3:a:g.rodola:pyftplib:0.5.0:*:*:*:*:*:*

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 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](#)