

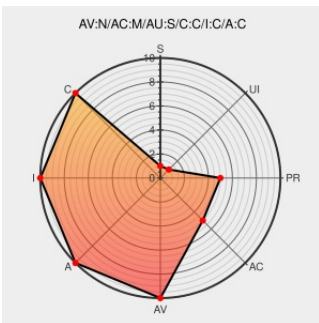


# CVE-2006-7094

Published on: 02/28/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

## CVE-2006-7094

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

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

ftpd, as used by Gentoo and Debian Linux, sets the gid to the effective uid instead of the effective group id before executing `/bin/ls`, which allows remote authenticated users to list arbitrary directories with the privileges of gid 0 and possibly enable additional attack vectors.

CVE-2006-7094 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **8.5 - HIGH**

Access  
Vector

**NETWORK**

Access  
Complexity

**MEDIUM**

Authentication

**SINGLE**

Confidentiality  
Impact

**COMPLETE**

Integrity  
Impact

**COMPLETE**

Availability  
Impact

**COMPLETE**

## CVE References

Description

Tags

Link

155317 – net-ftp/ftpd 0.17-r4 always runs ls with gid 0?

[Patch](#)  
[bugs.gentoo.org](#)  
[text/html](#)

[CONFIRM](#) [bugs.gentoo.org/show\\_bug.cgi?id=155317](https://bugs.gentoo.org/show_bug.cgi?id=155317)

CXSecurity - IDS

[securityreason.com](#)  
[text/html](#)

[CX](#) [SREASON 2330](#)

#384454 - ftpd: Does not handle symlink? NFS? home directory - Debian Bug report logs

[bugs.debian.org](#)  
[text/html](#)

[CONFIRM](#) [bugs.debian.org/384454](https://bugs.debian.org/384454)

No Description Provided

[osvdb.org](#)

[OSVDB 34242](#)

[Inactive Link](#) [Not Archived](#)

SecurityFocus

[www.securityfocus.com](#)  
[text/html](#)

[BUGTRAQ 20070220 /bin/ls with gid=0 in Debian linux-ftp](#)

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](mailto: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 |
| Operating System                              | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 4.0     | All    | All     | All      |
| Operating System                              | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 4.0     | All    | All     | All      |
| Application                                   | <a href="#">Ftpd</a>   | <a href="#">Ftpd</a>         | All     | All    | All     | All      |
| Application                                   | <a href="#">Ftpd</a>   | <a href="#">Ftpd</a>         | All     | All    | All     | All      |
| Operating System                              | <a href="#">Gentoo</a> | <a href="#">Linux</a>        | All     | All    | All     | All      |
| Operating System                              | <a href="#">Gentoo</a> | <a href="#">Linux</a>        | All     | All    | All     | All      |
| cpe:2.3:o:debian:debian_linux:4.0:****:*:*:*: |                        |                              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:4.0:****:*:*:*: |                        |                              |         |        |         |          |
| cpe:2.3:a:ftpd:ftpd:****:*:*:*:               |                        |                              |         |        |         |          |
| cpe:2.3:a:ftpd:ftpd:****:*:*:*:               |                        |                              |         |        |         |          |
| cpe:2.3:o:gentoo:linux:****:*:*:*:            |                        |                              |         |        |         |          |
| cpe:2.3:o:gentoo:linux:****:*:*:*:            |                        |                              |         |        |         |          |

No vendor comments have been submitted for this CVE