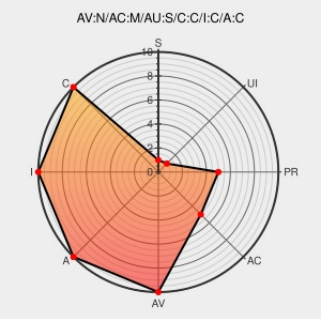
CVE-2006-7094

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	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
CXSecurity - IDS	securityreason.com, text/html	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
No Description Provided	osvdb.org, Inactive Link, Not Archived	OSVDB 34242
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20070220 /bin/ls with gid=0 in Debian linux-ftpd

Accepted linux-ftpd 0.17-23 (source i386) packages.qa.debian.org text/html CONFIRM packages.qa.debian.org/l/linux-ftpd/news/20061125T181702Z.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Ftpd	Ftpd	All	All	All	All
Application	Ftpd	Ftpd	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	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

← Previous ID Next ID→