

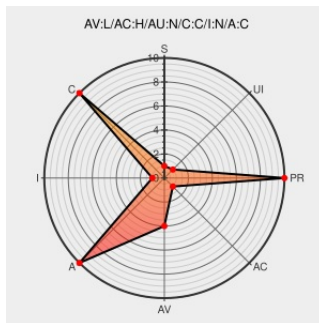


CVE-2005-4784

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4784

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

Certain versions of [Posix](#) from [Austin Group](#) contain the following vulnerability:

Multiple buffer overflows in the POSIX `readdir_r` function, as used in multiple packages, allow local users to cause a denial of service and possibly execute arbitrary code via (1) a symlink attack that exploits a race condition between `opendir` and `pathcon` calls and changes the filesystem to one with a larger maximum directory-entry name length,

or (2) possibly via programmer-introduced errors on operating systems with a small struct `dirent`, such as Solaris or BeOS, as demonstrated in packages including (a) gcj, (b) KDE, (c) libwww, (d) the Rudiments library, (e) teTeX, (f) xmail, (g) bfbtester, (h) ncftp, (i) netwib, (j) OpenOffice.org, (k) Pike, (l) reprepro, (m) Tcl, and (n) xgsmllib.

CVE-2005-4784 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

SecurityFocus

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

[BUGTRAQ 20051108 Re: readdir_r considered harmful](#)

`readdir_r` considered harmful

[Vendor Advisory](#)
womble.decadentplace.org.uk
[text/x-c](#)
[Inactive Link](#) [Not Archived](#)

[MISC womble.decadentplace.org.uk/readdir_r-advisory.html](#)

SecurityFocus

www.securityfocus.com

[BUGTRAQ 20051105 Re: readdir_r considered](#)

	text/html	harmful
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051105 Re: readdir_r considered harmful
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051106 Re: readdir_r considered harmful
Multiple Vendor ReadDir_R Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 15259
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051106 Re: readdir_r considered harmful
SecurityFocus	www.securityfocus.com text/x-c	BUGTRAQ 20051101 readdir_r considered harmful
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051106 Re: readdir_r considered harmful

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
Operating System	Austin Group	Posix	All	All	All	All
Operating System	Austin Group	Posix	All	All	All	All
cpe:2.3:o:austin_group:posix:*****::						
cpe:2.3:o:austin_group:posix:*****::						