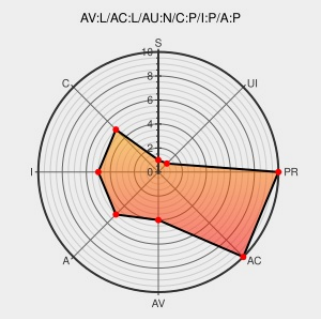
CVE-2006-1564

Published on: 03/31/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1564

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Untrusted search path vulnerability in libapache2-svn 1.3.0-4 for Subversion in Debian GNU/Linux includes RPATH values under the /tmp/svn directory for the (1) mod_authz_svn.so and (2) mod_dav_svn.so modules, which might allow local users to gain privileges by installing malicious libraries in that directory.

CVE-2006-1564 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
#359234 - libapache2-svn: modules have trapdoor rpath /tmp/svn - Debian Bug report logs	Exploit, Patch, bugs.debian.org, text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=359234
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF libapache2-svn-file-upload(25680)
Debian GNU/Linux Multiple Packages Insecure RUNPATH Vulnerability	Patch, cve.report (archive), text/html	BID 17288

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	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha	All
Operating System	Debian	Debian Linux	3.1	All	amd64	All
Operating System	Debian	Debian Linux	3.1	All	arm	All
Operating System	Debian	Debian Linux	3.1	All	hppa	All
Operating System	Debian	Debian Linux	3.1	All	ia-32	All
Operating System	Debian	Debian Linux	3.1	All	ia-64	All
Operating System	Debian	Debian Linux	3.1	All	m68k	All
Operating System	Debian	Debian Linux	3.1	All	mips	All
Operating System	Debian	Debian Linux	3.1	All	mipsel	All
Operating System	Debian	Debian Linux	3.1	All	ppc	All
Operating System	Debian	Debian Linux	3.1	All	s-390	All
Operating System	Debian	Debian Linux	3.1	All	sparc	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha	All
Operating System	Debian	Debian Linux	3.1	All	amd64	All
Operating System	Debian	Debian Linux	3.1	All	arm	All
Operating System	Debian	Debian Linux	3.1	All	hppa	All
Operating System	Debian	Debian Linux	3.1	All	ia-32	All

Operating System	Debian	Debian Linux	3.1	All	ia-64	All
Operating System	Debian	Debian Linux	3.1	All	m68k	All
Operating System	Debian	Debian Linux	3.1	All	mips	All
Operating System	Debian	Debian Linux	3.1	All	mipsel	All
Operating System	Debian	Debian Linux	3.1	All	ppc	All
Operating System	Debian	Debian Linux	3.1	All	s-390	All
Operating System	Debian	Debian Linux	3.1	All	sparc	All

cpe:2.3:o:debian:debian_linux:3.1:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:alpha:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:amd64:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:arm:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:hppa:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:ia-32:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:ia-64:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:m68k:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:mips:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:mipsel:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:ppc:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:s-390:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:sparc:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:alpha:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:amd64:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:arm:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:hppa:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:ia-32:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:ia-64:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:m68k:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:mips:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:mipsel:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:ppc:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:s-390:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:sparc:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→